

Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Previously presented) A method comprising:

determining at a first classifying forwarding element if a classification parameter is available for Internet Protocol security (IPsec) traffic that indicates a route for the IPsec traffic and classifying said traffic if available;

if said classification parameter is not available, and the IPsec traffic is encrypted then decrypting traffic in a decrypting forwarding element after said traffic has passed through said classifying forwarding element, and determining the classification parameter for the IPsec traffic at the decrypting forwarding element; and

forwarding the IPsec traffic based on the classification parameter.

2. (Previously Presented) The method of claim 1 further comprising receiving the IPsec traffic at the classifying forwarding element.

3. (Original) The method of claim 1 in which the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic.

4. (Original) The method of claim 1 in which the IPsec traffic includes a data packet.

5. (Original) The method of claim 1 further comprising forwarding other IPsec traffic included in a traffic stream with the IPsec traffic based on the classification parameter.

6. (Previously Presented) An article comprising:
a machine-readable medium which stores machine-executable instructions, the instructions causing a machine to:

determine at a first mechanism if a classification parameter is available for Internet Protocol security (IPsec) traffic that indicates a route for the IPsec traffic;

if a classification parameter is not available,
sending said traffic to a second mechanism after said traffic has passed said first mechanism, and which second mechanism decrypts the IPsec traffic if the IPsec traffic is encrypted and determine the classification parameter for the IPsec traffic at the second mechanism; and

forward the IPsec traffic based on the classification parameter.

7. (Original) The article of claim 6 further causing a machine to receive the IPsec traffic at the first mechanism.

8. (Original) The article of claim 6 in which the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic.

9. (Original) The article of claim 6 in which the IPsec traffic includes a data packet.

10. (Original) The article of claim 6 further causing a machine to forward other IPsec traffic included in a traffic stream with the IPsec traffic based on the classification parameter.

11. (Currently amended) A system comprising:

a classifying forwarding element configured to communicate with a network, to determine if a classification parameter that indicates a route for a traffic stream is available for a packet included in the traffic stream; and

a decryption forwarding element configured to receive the packet from the classifying forwarding element, to ~~decrypt~~ perform an encryption-related procedure on the packet if the packet is encrypted and associated with a known encryption-related key, and determine said classification parameter, if the classification parameter is available from

either of said forwarding elements, to forward the packet based on the route for the traffic stream.

12. (Previously Presented) The system of claim 11 further comprising a third mechanism configured to communicate with the classifying forwarding element and with the decryption forwarding element and to determine a classification parameter for the packet if a classification parameter is not available.

13. (Previously Presented) The system of claim 12 in which the second mechanism is also configured to forward the packet to the third mechanism if the packet is not associated with a known encryption-related key.

14. (Previously Presented) The system of claim 12 in which the third mechanism is also configured to, after determining the classification parameter for the packet, forward the classification parameter to the first mechanism.

15. (Previously presented) The system of claim 12 in which the third mechanism is also configured to, after determining the encryption-related key for the packet, forward the encryption-related key to the decryption forwarding element so that the decryption forwarding element can perform the encryption-related procedure.

16. (Cancelled)

17. (Currently amended) The system of claim 11 further comprising a plurality of additional mechanisms, each additional mechanism configured to communicate with the classification forwarding device to ~~encrypt~~ perform an encryption-related procedure on the packet if the packet is encrypted and associated with a known encryption-related key, and, if the classification parameter is available, to forward the packet based on the route for the traffic stream.

18. (Original) The system of claim 11 in which the packet includes an Internet Protocol security data packet.

19. (Original) The system of claim 11 in which the traffic stream includes a plurality of Internet Protocol security data packets.

20. (Original) The system of claim 11 in which the first mechanism is also configured to forward the packet to the second mechanism if the packet is encrypted.

21. (Original) The system of claim 11 in which the route for the traffic stream includes a route through a network.

22. (Original) The system of claim 21 in which the network includes an Internet.

23. (Currently amended) The system of claim 11 in which the encryption-related procedure includes encrypting the packet.

24. (Currently amended) The system of claim 11 in which the encryption-related procedure includes decrypting the packet.

25. (Original) The system of claim 11 further comprising another mechanism configured to receive the packet from the second mechanism and to forward the packet based on the route to an ultimate destination of the packet.

26. (Original) The system of claim 11 in which the first mechanism is also configured to route packets included in the traffic stream based on a load balancing scheme.

27. (New) A system, comprising:

a first classifying forwarding element in communication with a network, the first classifying forwarding element having an output;

a plurality of decrypting forwarding elements in communication with the output of the first classifying

forwarding element, each of the plurality of decrypting forwarding elements having an output;

a control element in communication with the first classifying forwarding element and the plurality of decrypting forwarding elements; and

one or more second classifying forwarding elements in communication with one or more outputs of the decrypting forwarding elements, the one or more second classifying forwarding elements different than the first classifying forwarding element, the one or more second classifying forwarding elements each having an output.

28. (New) The system of claim 27, further including one or more servers in communication with the output of at least one of the one or more second classifying forwarding elements.

29. (New) The system of claim 28, wherein the control element includes security information for the one or more servers.

30. (New) The system of claim 29, wherein the security information includes one or more access tokens.